IJTRET "Voice of Innovative Minds"
doi.org/10.54473/IJTRET.2021.5202
International Journal of Trendy Research in Engineering and Technology
Volume 5 Issue 2 April 2021
ISSN No 2582-0958

WIRELESS COMMUNICATION SYSTEM: SECURITY ISSUES

C.Lakshmi ,A.Rajiv
Assistant Professors,Department of ECE, Sriram Engineering College,Tamilnadu,India

ABSTRACT

In Modern Communication wireless communication uses MIMO technique to transmit and receive data. The data security is important in communication. The various cryptography algorithm are used to insure the security of wireless communication. The extensive literature review is conducted to study the various security issues in MIMO system

Key Words: Communication, MIMO, cryptography, data security

I.INTRODUCTION

In communication systems Data integrity and Authentication is important considerations .Wireless transmission system is more vulnerable to security issues. In wireless transmission system the signal is transmitted from transmitter to receiver by using antennas. In SISO systems communication channel has single input and single output, so only one intend receiver is used whereas in MIMO communication system multiple input and multiple outputs are present so it is difficult to transmit the signal to one intend receiver. In wireless systems the radio signals is act as transmission medium, each transmitter and receiver is tunned to particular frequency by using Frequency division multiple access(FDMA) technique.

The above figure depicts the basic elements in communication model. The information source is a signal to be transmitted ,which has encoder to encode the data that is compatible to communication channel. In receiver end the decoder decodes the data and retrieve the transmitted signal.

The communication channel not only transmit the simple messages but it transmits the secure data in military application, Medical data transmission etc.,. The medical images are transmitted in wireless communication medium such as patient MRI images and CT scan images. These data should be kept secret. But eavesdroppers interrupt the data and modify the contents. In order to ensure the secure transmission additional security system need to be added to the existing system.

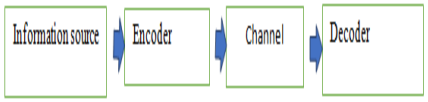

Figure 1: Basic Communication Model

Figure2:Single Input Single Output Communication model

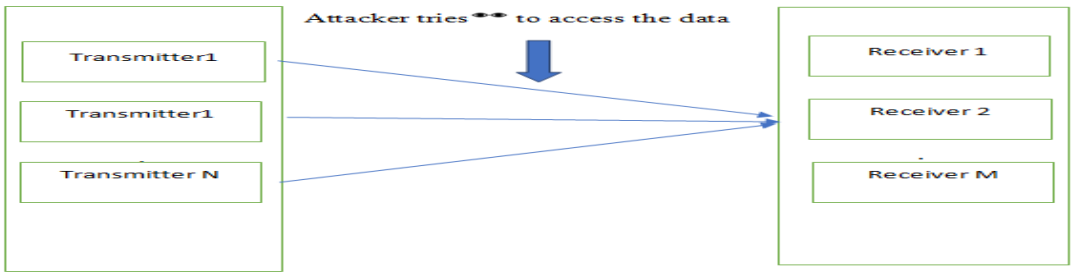

Figure 3:Multiple Input Multiple Output System with attacker scenario

In the above system when the attacker is introduced between transmitter and receiver. The various multiple access techniques such as time division multiple access ,space division multiple access, frequency division multiple access are used. The additional noise is introduced along with the data[1][2],so it reduces the attacker signal strength. The security is less when the number antennas used by the attacker is more than the number antenna used by the receiver.

The attacker not only try to access the data, it will also cause signal fading ,because of this issue the signal strength will be reduced before it reaches to receiver and unable to detect the signal.

The capacity of the channel also plays a vital in communication system.If transmission rate should be lesser than the capacity of the channel, probability of error is less. If the transmission rate is higher than the channel capacity the probability of error is high. Shannon derived the channel capacity theorem, that follows

$$C = B\log_2(1+S/N) \quad (1)$$

Where C is the capacity of the channel, B is the bandwidth and S/N is the signal to noise ratio.

II.EXISTING WORK

As we discussed earlier, consider the model has N transmitters and M receivers. In [2] X number of transmitters transmits the signal and N-X transmitter transmits the noise. When the attacker has Y antennas where Y is lesser than M,the security is more. If Y is greater than M,the system doesn't guarantee the security.

Yiliang et al [3] discussed the drawback of existing AN :Artificial Noise models and proposed the novel scheme to increase the security. In all the existing models AN is introduced so the attacker signal strength is reduced, where the AN is added by using unused transmitters called null spaces. In this paper the null spaces are chosen based on the eigen values. By using Wish art matrix, the larger eigen values are chosen as the message sending sub channels and remaining sub channels are chosen as Noise sending sub channels. In this method the security increases by 20%-40% of existing methods. The advantage of this method is the noise added along with the message so the attacker get confuse ,not possible to distinguish between noise and message. The receiver identifies the message by using precoder.

In MIMO system there may be more than one eavesdropper present in the network attack the channel.The power allocation takes place a vital role in secure communication channel.The available power is allocated between the message transmission and artificial noise is transmission. Allocation of inappropriate power causes the channel security, so the amount of power allocation to the message and noise should be pre-determined.

Shang-Ho Tsai et al [4] proposes the effective power allocation scheme to enhance the security. The power allocation is based on the SNR of the channel. If more power allocated to artificial noisein low SNR channel causes the security degradation. In this paper the author considers the both scenario that the MIMO system having single eavesdropper and MIMO system having multiple eavesdropper.

Now the method of using AN in the communication channel have some disadvantages, so the cryptography algorithm is implemented in wireless communication channel to increase the security. The security issues like Man in the middle attack will be well addressed in this method. There are various cryptography algorithms are available like ECC,RSAetc.,. The ECC is most common used algorithm because the security and computation speed is high compare other existing algorithms.

III.ANALYSIS OF ECC ALGORITHM IN WIRELESS COMMUNICATION CHANNEL

It is easy to implement Elliptic curve cryptography in hardware and software. The Elliptic curve Diffie Helmen Key exchange and Elliptic curve Digital signature scheme are used in wireless communication for security purpose [5]. The author proposed the ECC based key establishment protocol gives more security, man in the middle attack is introduced and the security of the communication channel is analysed.

(a). Elliptic curve Diffie Helman Key Exchange scheme

In ECDH algorithm the transmitter and receiver generate the two different keys based on the two different random numbers and finally the two keys are compared. If both the keys are same then the message is secure otherwise the message is lost.

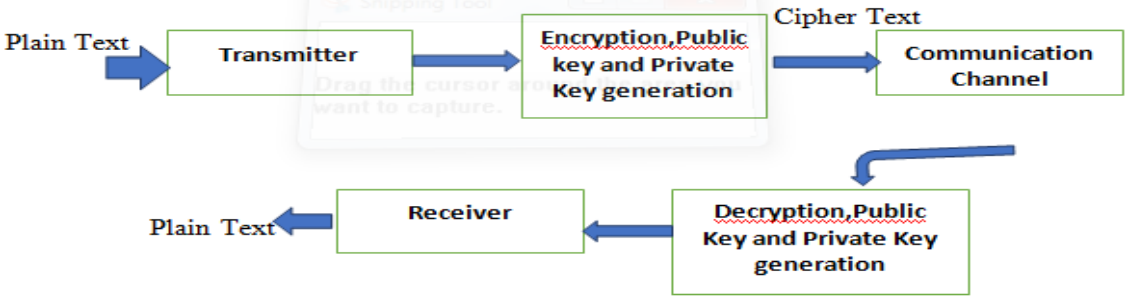

Figure 4: Mechanism involved in ECDH Algorithm

***Algorithm*:**

1.Transmitter generates the Private key K_t and Public Key KP_t.$KP_t=K_tP$,Where P is the base point on the Elliptic curve.

2.Receiver generates Private key $K_r$and KP_r Public key.$KP_r=K_rP$.

3.The transmitter calculates the Key K= $K_t*KP_r$and receiver calculates the Key= K_r*KP_t

4.The private keys K_t and K_r are not shared in the communication channel, so the attacker like Man in the middle attack not able to decrypt the message.

In this method, the certificate authentication is not provided so the attacker can intercept the transmitted message.

(b).Signature Based Algorithm

Signature based authentication is most powerful than Key exchange algorithm. This algorithm Comprises of three steps: 1.key generation 2. Signature Generation 3. Signature Verification

Key generation:

Consider the any point on the elliptic curve P(x.y)

1.The random number is chosen such that d. This is consider as a private key.

2.The public k key is computed Q=dP

Signature generation:

Signature generation is carried by the transmitter side.

1.The random number is k chosen such that the r should be equal to zero.If so chose another

2.Compute kP

3.Compute r=kP.x mod n

4.Compute $s=k^{-1}(h(m)+dr)$, whereh(m) is a hash function.

The signature is created on message is (r,s)

Signature Verification:

1.Compute $d=s^{-1}$ mod n

2.Compute $U_1=h(m)$ d mod n

3.Compute $U_2=ry$ mod n

4.Compute R= $U_1P+ U_2 Q$

5.Calculate v=R.x mod n

6.Accept the message if r=v

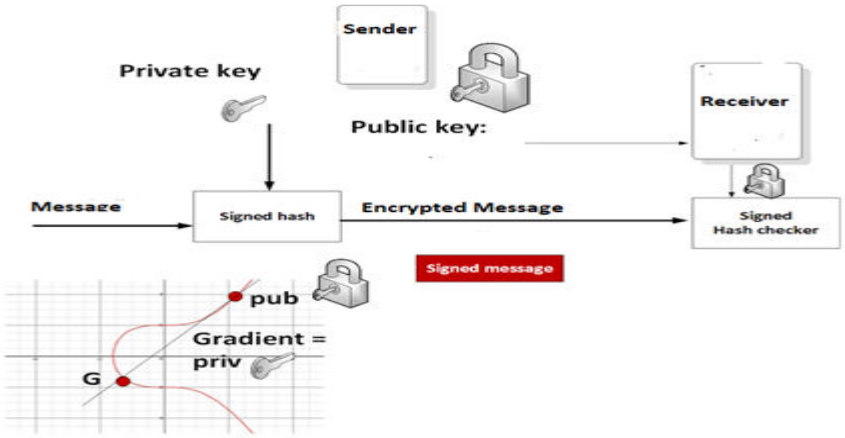

Figure 5:Mechanism involved in Signature based Algorithm

Zhang Juan et al [6] proposes the ECC algorithm based on certificate Authority scheme. The certificate authority CA issues the CertA for transmitter, A denotes transmitter. CertA consists of Transmitter identity, Transmitter public key, pair of keys denoted the transmitter, the hash function and the other useful information such as time, date needed for certificate authentication. In this method certificate of transmitter and receiver is mutually exchanged, so the transmitter authenticates the receiver's certificate and receiver authenticates the transmitter's certificate. If both the certificates are authenticated then only the message is accepted. Like key exchange elliptic curve cryptography in this method also the public key is exchanged, private key is kept confidential. In this protocol key is generated for every session so it is not possible to obtain the newly generated key by the eavesdropper.

4.CONCLUSION

This paper analyses various existing methods for wireless channel security. In some channels the security is provided by adding Artificial noise and some channel the cryptography algorithms are implemented. The artificial noise is added to the channel to confuse the attacker , but increases the signal power. In wireless channel power is the influencing factor. The cryptography method the cryptography algorithm is used to provide the security and most common algorithm is ECC based security. In ECC algorithm two possibilities are available. ECC key exchange mechanism which ensures less security than signature based ECC algorithm. The signature based algorithm also vulnerable to security threats.So, the hardware-based security is proposed along with complex hash algorithm like kurosawadesmedt algorithm key encapsulation mechanism.

REFERENCES

1. Q. Li and L. Yang, "Artificial Noise Aided Secure Precoding for MIMO Untrusted Two-Way Relay Systems With Perfect and Imperfect Channel State Information," in *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 10, pp. 2628-2638, Oct. 2018.

2. X. Chen, L. Pang, Y. Tang, H. Yang and Z. Xue, "Security in MIMO wireless hybrid channel with artificial noise," *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, Shanghai, 2015, pp. 1-4.

3. Y. Liu, H. Chen and L. Wang, "Secrecy Capacity Analysis of Artificial Noisy MIMO Channels—An Approach Based on Ordered Eigenvalues of Wishart Matrices," in *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 617-630, March 2017.

4. S. Tsai and H. V. Poor, "Power Allocation for Artificial-Noise Secure MIMO Precoding Systems," in *IEEE Transactions on Signal Processing*, vol. 62, no. 13, pp. 3479-3493, July1, 2014.

5. Liu Yongliang,Wen Gao1, Hongxun Yaoand Xinghua Yu "Elliptic Curve Cryptography Based WirelessAuthentication Protocol" *International Journal of Network Security*, Vol.5, No.3, PP.327–337, Nov. 2007

6. J. Zhang and F. Deng, "The Authentication and Key Agreement Protocol Based on ECC for Wireless Communications," *2009 International Conference on Management and Service Science*, Wuhan, 2009, pp. 1-4.